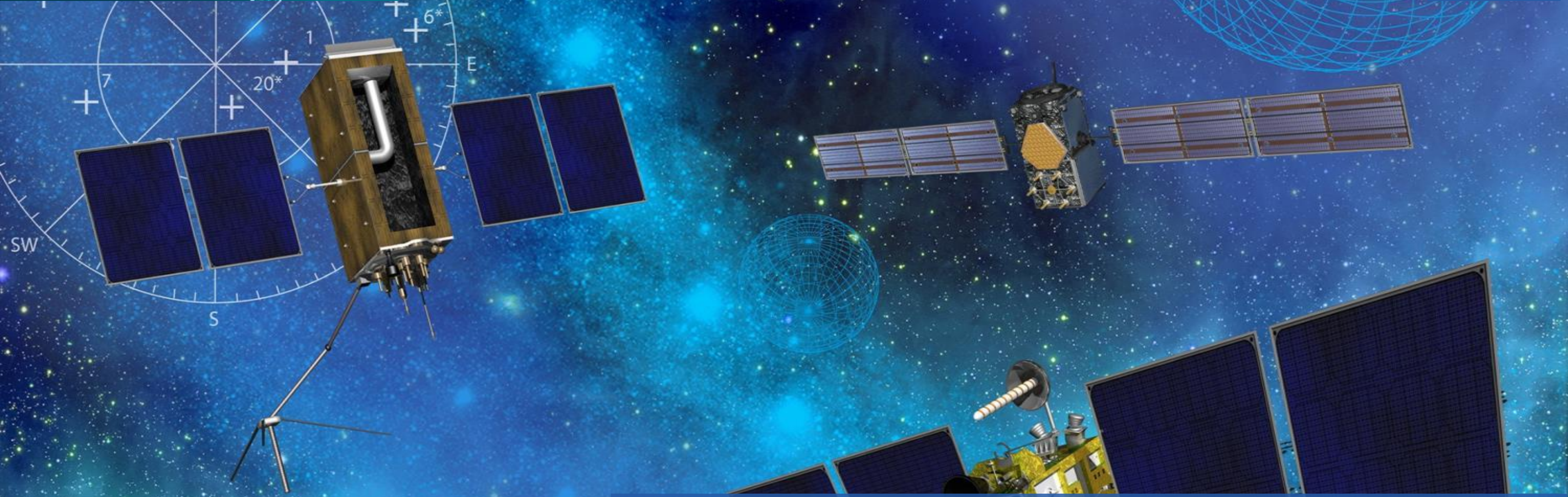
WORKSHOP ON SYNCHRONIZATION AND TIMING SYSTEMS

THE (R)EVOLUTION CONTINUES:
TIME FOR TOMORROW'S WORLD

JUNE 18-21, 2018
SAN JOSE, CA
DOUBLETREE SAN JOSE

atis

SPIRENT



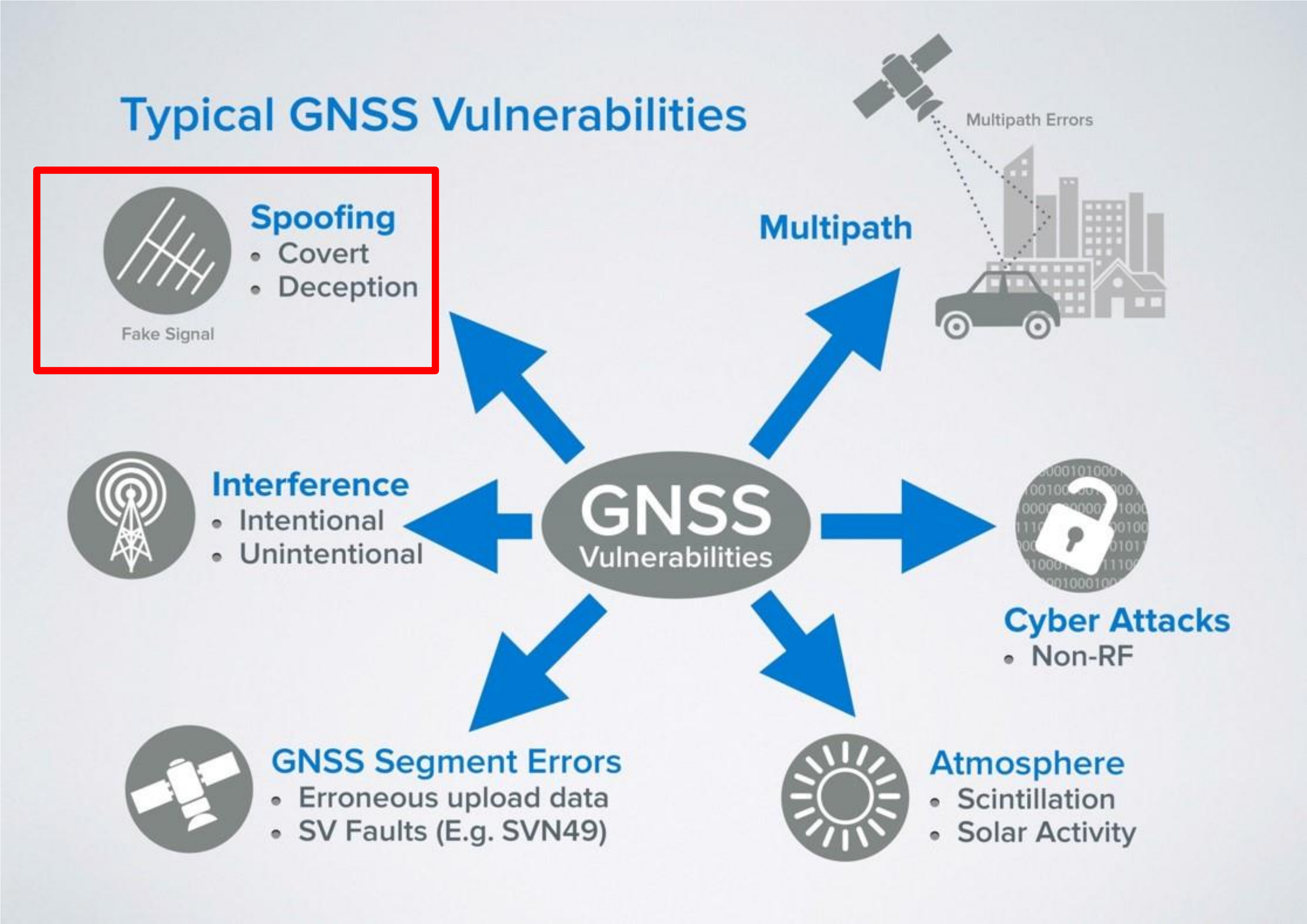
Time-Spoofing of GNSS Receivers: Lessons Learned and Mitigation

By Guy Buesnel, CPhys, FRIN

Spirent Communications, June 2018

Real world threats to GNSS

Impacting Time and Position



Typical GNSS Vulnerabilities

GNSS Vulnerabilities

Spoofing
- Covert
- Deception

Fake Signal

Multipath

Multipath Errors

Interference
- Intentional
- Unintentional

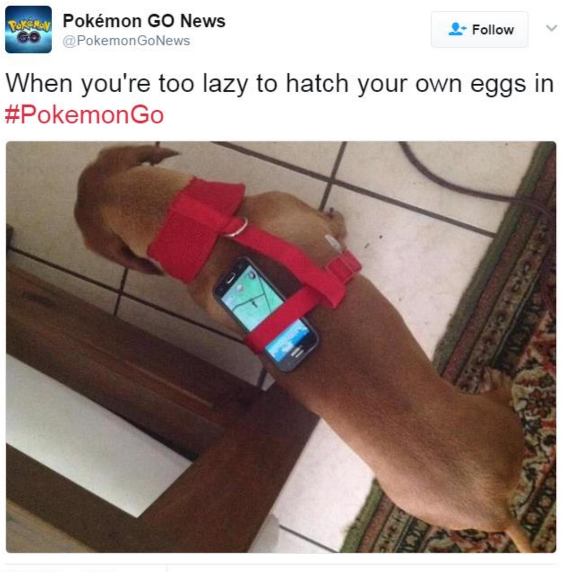
Cyber Attacks
- Non-RF

GNSS Segment Errors
- Erroneous upload data
- SV Faults (E.g. SVN49)

Atmosphere
- Scintillation
- Solar Activity

GPS Spoofing – emergence as real threat

- Pokémon GO… When gamers discovered spoofing…..

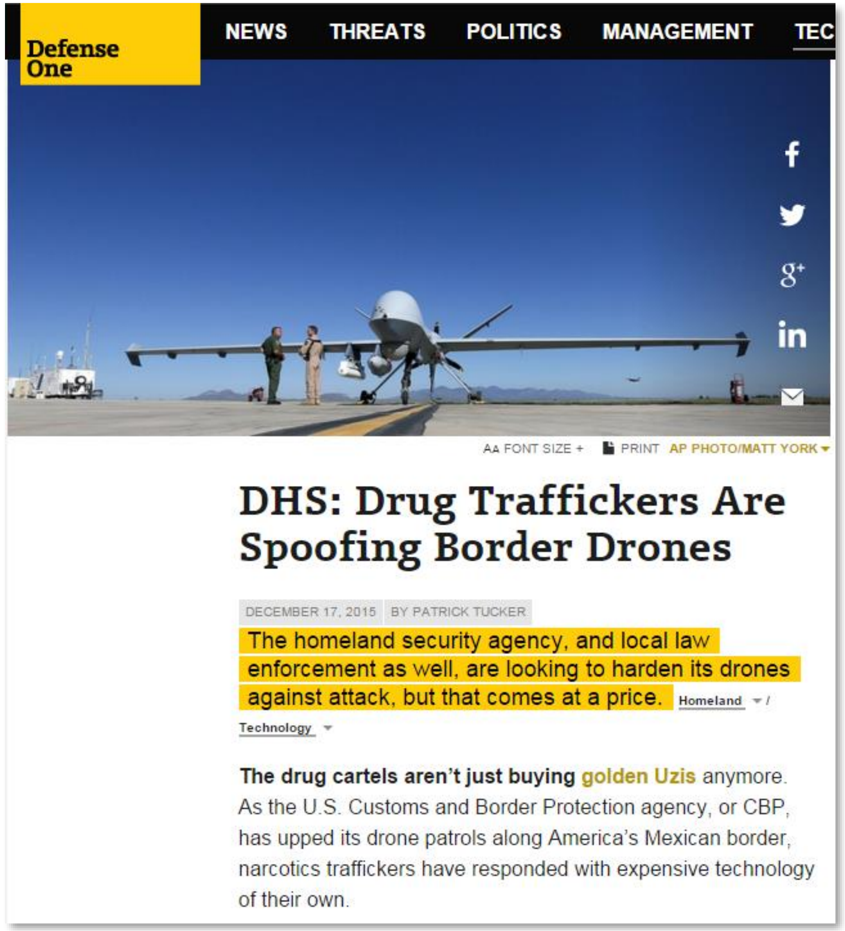


Pokémon GO News
@PokemonGoNews

When you're too lazy to hatch your own eggs in #PokemonGo

Six weeks from primitive to Sophisticated….

GPS Spoofing – emergence as real threat



DHS: Drug Traffickers Are Spoofing Border Drones

DECEMBER 17, 2015 BY PATRICK TUCKER

The homeland security agency, and local law enforcement as well, are looking to harden its drones against attack, but that comes at a price. Homeland / Technology

The drug cartels aren't just buying golden Uzis anymore. As the U.S. Customs and Border Protection agency, or CBP, has upped its drone patrols along America's Mexican border, narcotics traffickers have responded with expensive technology of their own.

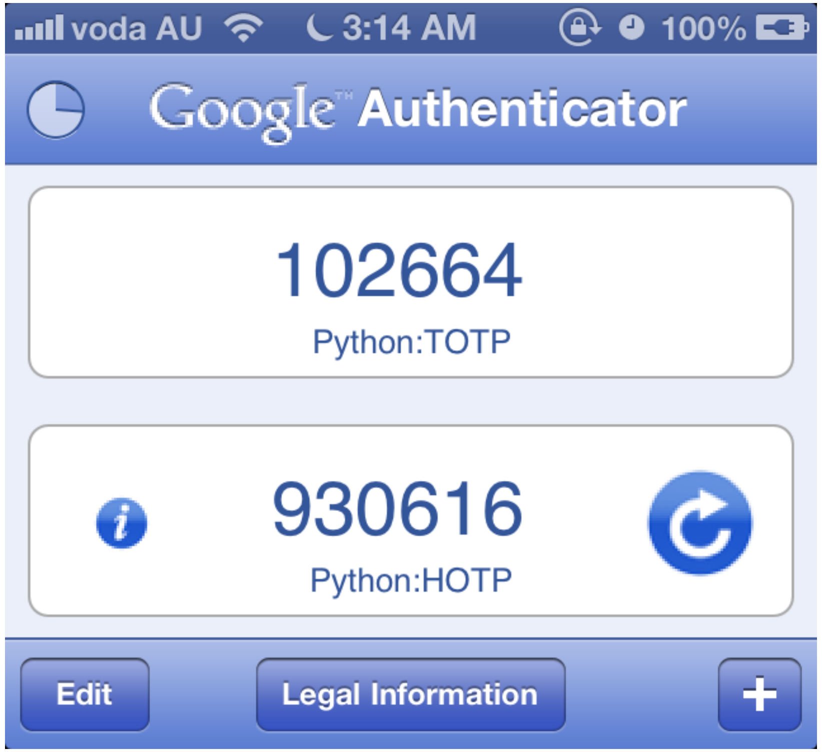
Reported in press 17th December 2015

- Highlighted attempts to jam and spoof drones patrolling US/Mexico border
- Attempted GPS spoofing in the real world reported for the very first time
- Criminals using technology to attempt to disrupt GNSS

Spoofing – Real world reports from 2017

DEFCON 25, August 2017, Caesar's Palace

- How to spoof NTP using a programmed SDR
- Masterclass in Time based one time password (TOTP) manipulation using time spoofing
- Spoofing GPS signals indoors is easy
  - GPS enabled equipment will often acquire the first signals it receives



102664

Python:TOTP

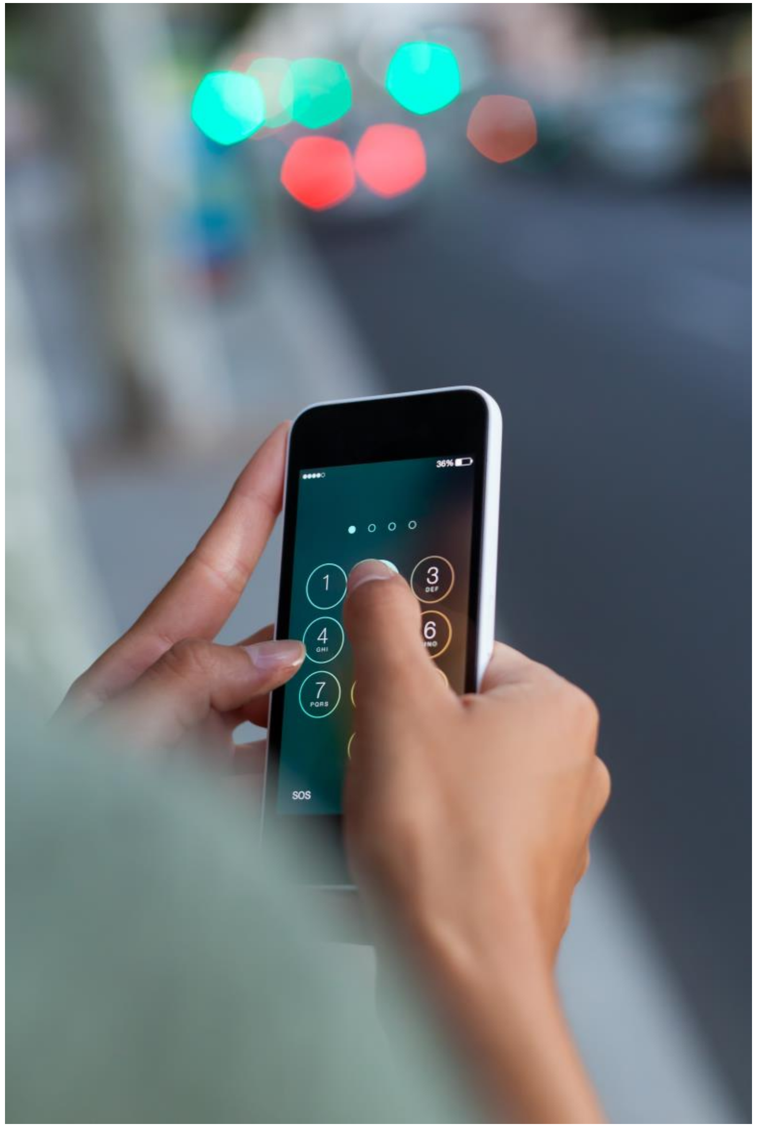
930616

Python:HOTP

Spoofing – Real world reports from 2017

September 2017 – ION GNSS+, Portland Convention Centre, Oregon

- Thursday 28th September - Multiple incidents of smartphones erroneously indicating incorrect time and position as reported by numerous users
- **Time in the past,** position showing as somewhere in Europe



Logan Scott has published an analysis of the event – *Spoofing Incident Report: An Illustration of Cascading Security Failure* – in Inside GNSS

Spoofing – Real world reports from 2017

- One kind of phone more affected than other brands/types
- Carriers included all the majors
- Whilst there was no GPS signal in the exhibition hall, there was cellular coverage and many wi-fi points
- Clues to smart phones that the leaked signals were not authentic
  - Large date/time shift
  - Large location shift (several thousand miles)
- Relatively unsophisticated attack – but numerous devices affected
- Spoof date/time was 12 January 2014 – where devices accepted this data, this caused problems with data (email, text messages, etc)

Spoofing – Detection/Mitigation strategies

- Risk Assessment vital to identify most cost effective strategies based on quantitative data
- Improved Antenna Technologies can make a big difference
- Processing (some of the ways to detect a spoofer)
  - Monitor power levels
  - Monitor own position
  - Look for code/carrier range changes or inconsistency
  - Navigation data analysis
  - Jump detection

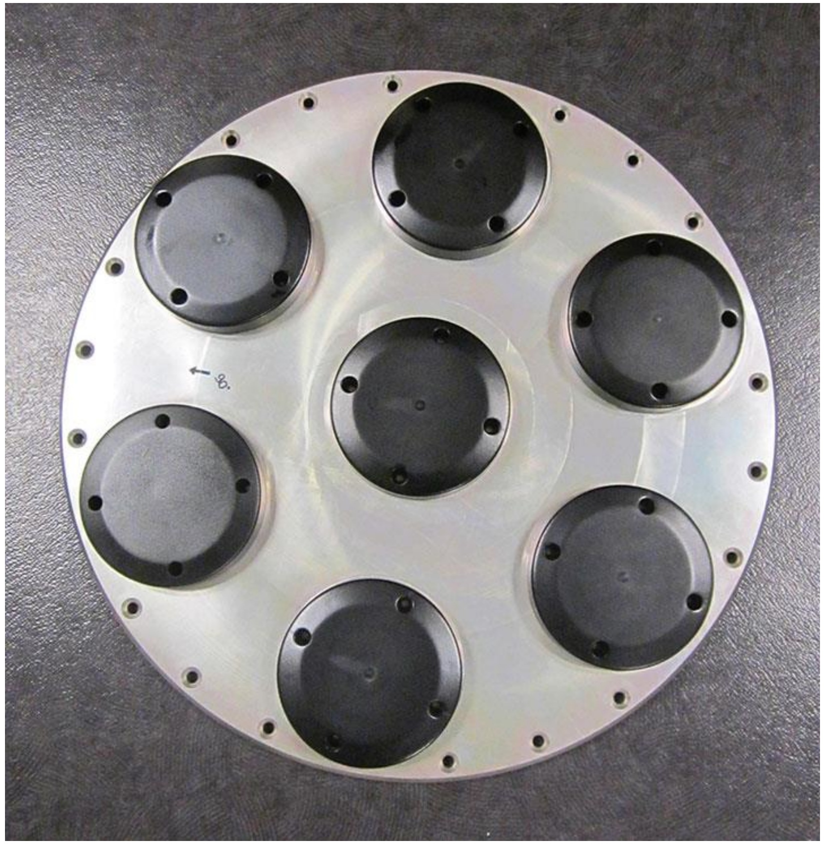


Image courtesy of GPS World

Hackers talk about GPS spoofing…

GPS Spoofing “…so it is now party trick simple and cheap - This is the big game changer from the past” – **“Karit”, Defcon 25, 2017**

“…..NMEA is simply text over rs232. If you plug a terminal into your AIS transmitter you can tell people anything you like. A lot simpler than interfering with GPS.” - **Unknown contributor, Schneier On Security blog…**

Image courtesy Hackaday

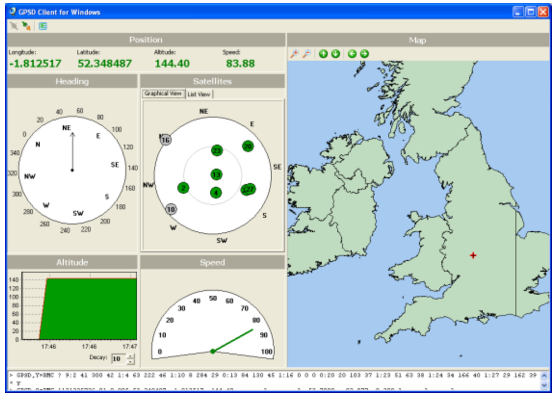
Cyber-Security Considerations for GNSS

“Attack Surface”

- GNSS solutions utilise existing computing technologies
  - Many GNSS receivers run embedded operating systems (VxWorks, Linux etc.)
  - User interface, logging & alerting components run on “off the shelf” hardware & operating systems (embedded computers & processors, mobile devices, Windows, Android etc.)
  - Communication protocols such as TCP/IP, USB and RS232 move data between devices.
  - The Internet, Local & Wide Area Networks provide access to remote systems & data sources.

Image Courtesy of Pakwheels

Image Courtesy of Adaptek Automation Technology



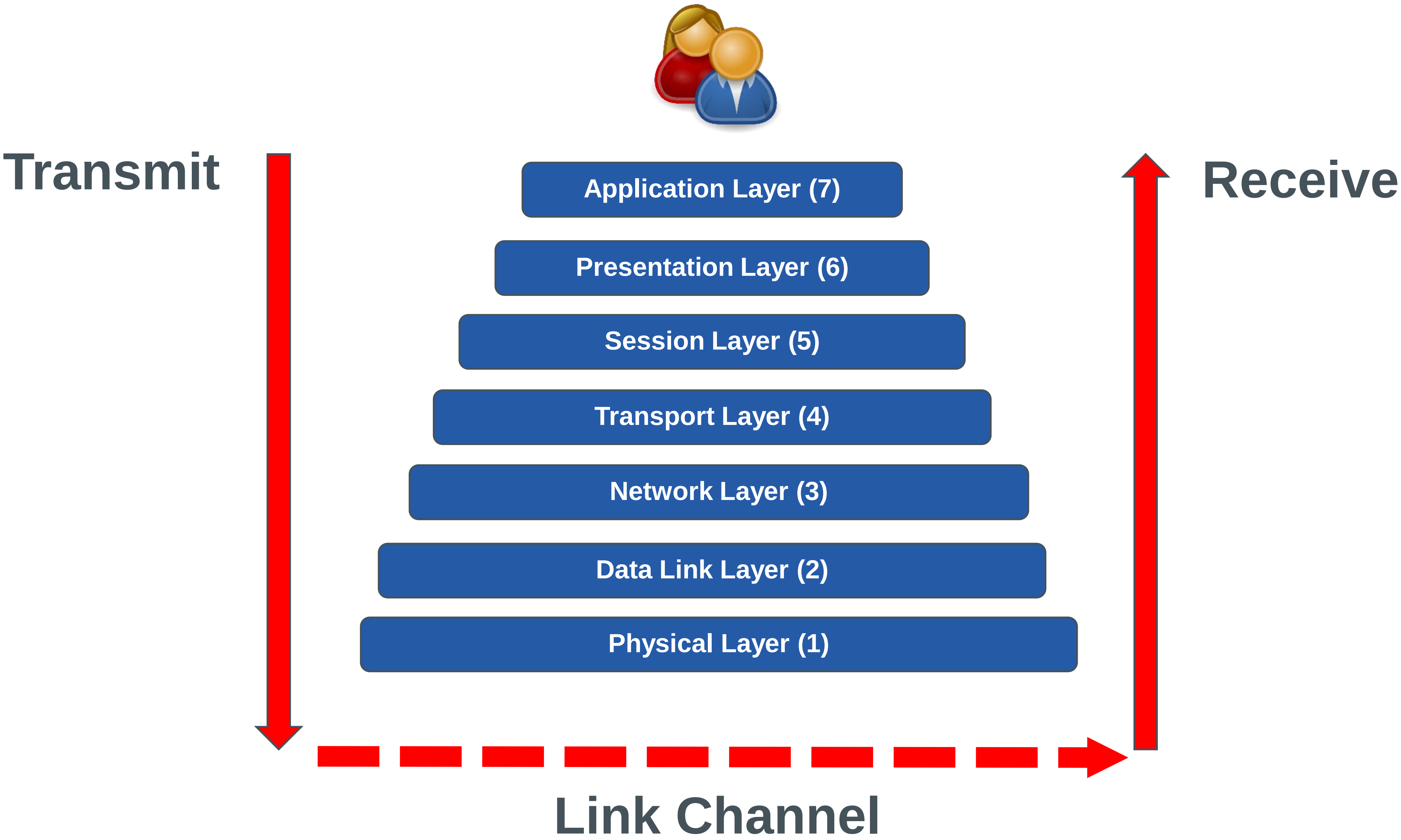
Longitude: -1.812517 Latitude: 52.348487 Altitude: 144.40 Speed: 83.88

Decay: 10

```
> GPSD,Y=RMC ? 9:2 41 300 42 1:4 63 222 46 1:10 8 284 29 0:13 84 130 45 1:16 0 0 0 0:20 20 103 37 1:23 51 63 38 1:24 34 166 40 1:27 29 162 39
< y
```

Image Courtesy of Logical Genetics

7-Layer OSI Model



Transmit

Application Layer (7)

Presentation Layer (6)

Session Layer (5)

Transport Layer (4)

Network Layer (3)

Data Link Layer (2)

Physical Layer (1)

Receive

Link Channel

Cyber-Security Considerations for GNSS

Firmware Attacks

- Malicious modification of code running on embedded devices within GNSS components e.g. microcontrollers, Field Programable Gate Arrays (FPGAs) etc

Image Courtesy of Apixel IT Support

- Applies to layers 1 & 2, but also other layers if the device is responsible for networking, user interfaces etc.
- Can be triggered in much the same way as Hardware Trojans.
- Difficult to detect, as firmware is usually inaccessible to the user
- Mitigations – code signing / secure boot features, code reviews and verification

Cyber-Security Considerations for GNSS

Hardware Attacks

- Attacking the low-level electronic components of a GNSS system (layers 1 & 2).
- “Hardware Trojan” - malicious modification of electronic components. Usually triggered once a pre-defined condition is reached, or a signal received.
  - Manipulation of data travelling on electrical busses i.e. spoofing, packet injection etc.
  - Preventing communication between legitimate components i.e. Denial of Service (DoS)
  - Leaking of sensitive information via radio or other signals.
- Difficult to detect – requires visual inspection or forensic analysis.
- Mitigation – tamper evident seals, sourcing electronic components and devices from reputable manufacturers, inspection of manufacturing processes.

Spoofing navigation data

NMEA

e.g., $GPGGA,**123519**,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,*47

NMEA Sentence type

Time of fix

Checksum

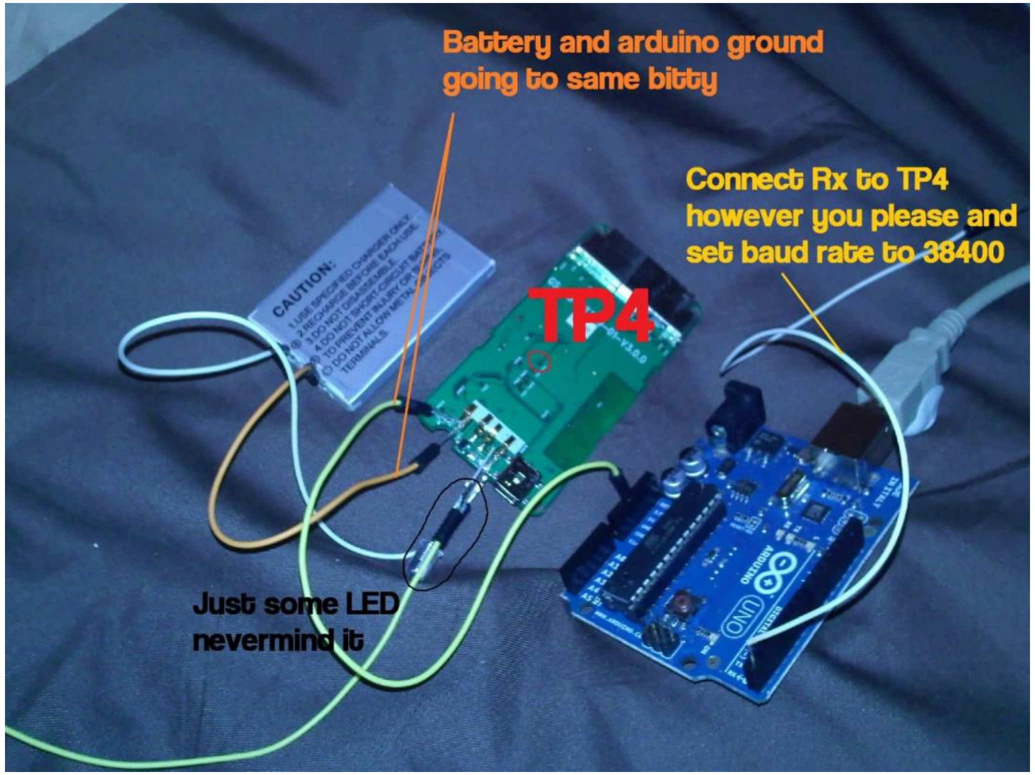

Battery and arduino ground going to same bitty
Connect Rx to TP4 however you please and set baud rate to 38400
TP4
Just some LED nevermind it

Image courtesy Arduino online forum:
https://forum.arduino.cc/index.php?topic=78774.0

Other NMEA Sentences include:-

- AAM - Waypoint Arrival Alarm
- ALM - Almanac data
- APA - Auto Pilot A sentence
- APB - Auto Pilot B sentence
- BOD - Bearing Origin to Destination
- BWC - Bearing using Great Circle route
- DTM - Datum being used.
- GGA - Fix information
- GLL - Lat/Lon data
- GRS - GPS Range Residuals
- GSA - Overall Satellite data
- GST - GPS Pseudorange Noise Statistics
- GSV - Detailed Satellite data
- RMB - recommended navigation data for gps
- RMC - recommended minimum data for gps
- RTE - route message
- TRF - Transit Fix Data
- STN - Multiple Data ID
- WCV - Waypoint closure velocity (Velocity Made Good)
- WPL - Waypoint Location information
- XTC - cross track error
- XTE - measured cross track error
- ZTG - Zulu (UTC) time and time to go (to destination)
- ZDA - Date and Time

Spirent experiences

Issues seen in user equipment

- Premature implementation of Leap Second Events
- Week Number Rollover- next one due in April 2019 (Modulo 1024 number)
- April 2014 GLONASS outage, corrupt ephemeris data
- Jan 2016 GPS timing errors due to incorrect ICD implementation in many GPS receivers (BBC DAB transmitters affected)
- Bit error events
- Sky obscuration
- Poor antenna installation
- Cross-over locations
- Dateline, equator, poles
- Spoofed signals (lack of detection, acceptance of incorrect pseudoranges and/or nav data)
- Interference (output of misleading data in band and out of band)
- Atmospherics – some effects in UK during event in 2015 affected telecoms transmitters

- **RF related**
- **Non-RF related**

Spirent Positioning and Timing Insights

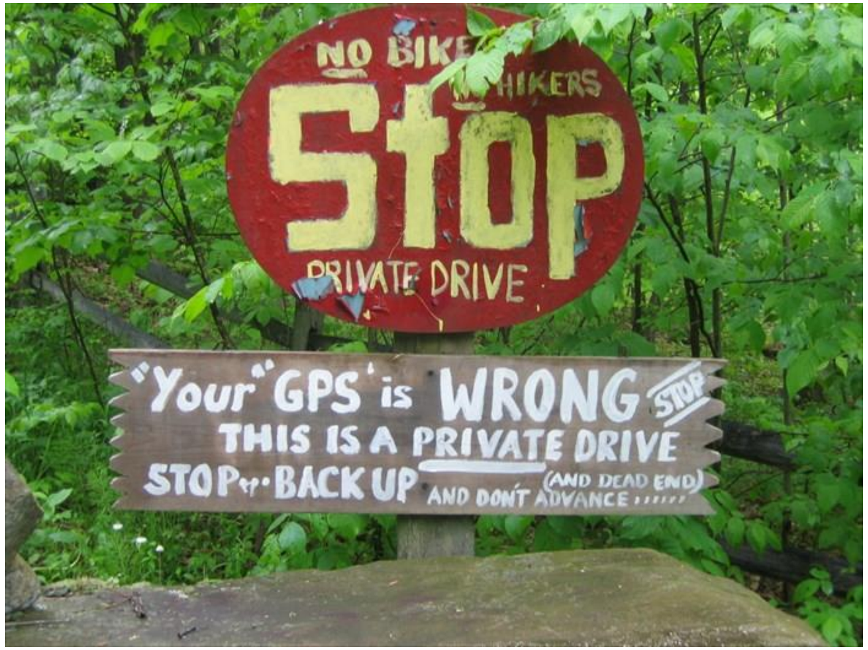
- Often not enough testing is conducted up-front and with many scenarios, live sky testing is not sufficient..
- Risk Assessment and knowledge of your operating environment is essential
- Build security into the design of timing systems right from the start
- There is a need to responsibly create awareness in many application segments
- *“GPS is more computer than radio”; “GPS Receivers lack cyber resilience. This is a National Issue.”* - Harold (“Stormy”) Martin, National Co-ordination office for Space based PNT

Image courtesy vinnews.com

Image courtesy "The Brofessional"

Image courtesy “New York Daily News)

Image courtesy MAIB



Thank you for listening

guy.buesnel@spirent.com

http://www.spirent.com/Solutions/Robust-PNT

Acknowledgements: My colleague David Smith for providing expert Cyber-Security knowledge, David Robinson (AKA “karit”,) ZX Security, for material on Spoofing NTP time

Join the GNSS Vulnerabilities group on Linked In to find out more about GNSS jamming and spoofing